

REMARKS

Reconsideration and allowance are respectfully requested in light of the above amendments and the following remarks.

A new Abstract is submitted herewith as required by the Office Action.

Claim 17 has been canceled, claims 1-3, 9, 13-16, 18-20, 22, and 26-28 have been amended, and claims 30-37 have been newly added. Support for the subject matter of the amended claims is provided in the original claims and the specification on page 3, lines 22-25, and page 4, lines 26-29. The amendments of claims 2, 3, 9, 14-16, 18-20, 22, and 26-28 were made to provide a proper antecedent basis or greater clarity for the features recited therein.

Claims 13-15 were rejected, under 35 USC §102(e), as being anticipated by Thomlinson et al. (US 6,389,535). Claims 1-12 and 26 were rejected, under 35 USC §103(a), as being unpatentable over Chasko et al. (US 6,715,078) in view of Schneck et al. (US 2001/0021926). Claims 16-25 were rejected, under 35 USC §103(a), as being unpatentable over Thomlinson in view of Schneck. Claims 27-29 were rejected, under 35 USC §103(a), as being unpatentable over Schneck in view of Nakamura et al. (US 6,415,371). To the extent these rejections may be deemed applicable to the amended and newly added claims, Applicants respectfully traverse.

Claim 1 now recites:

A data processing system for generating a key protection certificate comprising:

a PSD further comprising a unique device name, cryptography means, data processing means, data storage means and communications means;

wherein said cryptography means includes an asymmetric cryptographic key pair generating algorithm, a first securely shared secret key, a second securely shared secret key, symmetric cryptography means, a concatenation algorithm, a message authentication code algorithm, cryptographic seed information, a key protection certificate generating algorithm and a signing algorithm;

and wherein said key protection certificate generating algorithm comprises means for producing sequentially with said cryptographic key generating algorithm, upon completion of cryptographic key generation and in dependence on said generated cryptographic key, a unique digital certificate that comprises said unique device name.

The applied references fail to disclose or suggest the feature recited in claim 1 of a key protection certificate generating algorithm that produces, in dependence on a generated cryptographic key, a unique digital certificate that comprises the unique device name of a PSD. In an exemplary, but non-limiting, embodiment of the invention illustrated in Fig. 2, a generated digital certificate 20 includes both encrypted and unencrypted versions of a unique device name 65. The unencrypted version of the device name included within digital certificate 20 is identified by reference character 65 and the encrypted version included therein is identified as a signed device name 210.

Claim 1 recites a digital certificate having both encrypted and unencrypted information. The encrypted information is the information that is dependent on a generated cryptographic key. The unencrypted information is the unique device name for the PSD.

By contrast to the noted claimed feature, Chasko teaches in Fig. 4 a method 400 for creating a master key storage (MSK) key that includes only an encrypted version of a device's serial number (Chasko col. 6, lines 43-45 and 52-56). According to this method, a first random seed is generated (S402) by the manufacturer of a consumer transaction terminal (CTT) (col. 6, lines 45-47). The first random seed is sent (S404) to a cryptographic smart card 114, which generates (S406) a second random seed in response to receiving the first random seed (col. 6, lines 47-51). Cryptographic smart card 114 combines (S408) the second random seed, a serial number 202 of cryptographic smart card 114, and a serial number 203 of the device (col. 6, lines 51-56). Then, cryptographic smart card 114 generates (S410) an MSK key 206 by encrypting the combined second random seed, cryptographic smart card serial number, and device serial number with the first random seed, and the MKS key is stored (S412) in the cryptographic smart card (col. 6, lines 56-60). Thereafter, the cryptographic smart card permanently erases

(S414) all of the residues associated with the generation of the MSK key, and the process ends (col. 6, lines 60-64).

In summary, Chasko teaches creating an MSK key that includes only an encrypted version of a device's serial number. Chasko does not suggest producing a unique digital certificate that comprises an unencrypted version of a unique device name, as required by claim 1.

With the claimed digital certificate, a device receiving the certificate may extract the unencrypted version of the unique device name to find a match for this name and thereby determine an associated decryption key to use for decrypting the encrypted portion of the certificate. This is not possible with Chasko's system because all information within the MSK key is encrypted. Chasko's receiving device must know which decryption key to use for decrypting the MSK key without reference to the information within the MSK key.

Schneck also does not teach or suggest the above-mentioned feature of claim 1. Moreover, Schneck does not teach or suggest anything regarding the generation of a key protection certificate. Instead, Schneck teaches extracting a first decryption key from a certificate for use in decrypting an encrypted version of a second decryption key (see Schneck page 12, ¶188). The second decryption key may then be used to decrypt

a list of rules that are applied in governing a user's access to information associated with a packaged product (see page 13, ¶224). However, these features are not similar to the feature recited in claim 1 of producing a unique digital certificate that comprises an unencrypted version of a unique device name.

In accordance with the above discussion, Applicants submit that the applied references do not suggest the noted subject matter defined by claim 1. New claims 30 and 32 similarly recite the feature distinguishing claim 1 from Chasko and Schneck. Therefore, allowance of claims 1, 30, and 32 and all claims dependent therefrom is warranted.

Claim 13 has been amended to incorporate the features originally recited in claim 17. The combined teachings of Thomlinson and Schneck fail to disclose or suggest the feature now recited in claim 13 of selecting keys, algorithms, and reference parameters associated with a certificate by use of a PSD's unique device name that is contained in the certificate. As discussed above in connection with claim 1, a device receiving a certificate of this type may extract the unique device name to find a match for this name in a database and thereby determine an associated decryption key to use for decrypting an encrypted portion of the certificate.

By contrast to this noted feature, Thomlinson discloses encrypting a single master key, which is used to encrypt all of a user's data items, based on the user's password (Thomlinson col. 10, lines 17-19). By doing so, only the master key needs to be re-encrypted when a user changes his password, rather than having to re-encrypt all of the user's data items with multiple keys (col. 10, lines 19-22).

More specifically, Thomlinson discloses that an encryption provider derives a user key from a user-supplied password and uses the user key to decrypt a master key and a master authentication key (col. 10, lines 5-9). The master authentication key is used in conjunction with a specified message authentication code (MAC) to verify that the master key was decrypted correctly (col. 10, lines 9-11). The master key is then used to decrypt an appropriate item key and a corresponding item authentication key (col. 10, lines 11-13). The item authentication key is used in conjunction with the MAC to verify that the item key was decrypted correctly, and the item key is then used to decrypt the actual data item (col. 10, lines 13-16).

As may be determined from Thomlinson's disclosure discussed above, Thomlinson does not suggest selecting keys, algorithms, and reference parameters associated with a certificate by use of a PSD's unique device name that is contained in the certificate,

as recited in claim 13. And Schneck does not supplement Thomlinson's teachings in this regard.

Schneck teaches a cryptographically sealed certificate that is issued by an authorized Certification Authority (CA) and includes therein a decryption key issued by that CA (Schneck ¶187). In some preferred embodiments, a rule-encrypting key K_R is encrypted using an encryption key corresponding to the decryption key included in the certificate (Schneck ¶188). To obtain K_R , a device must have the decryption key that was stored in the certificate by the CA (Schneck ¶188). After the rule-encrypting key K_R is obtained, it may then be used to decrypt a data key K_D , within a packaged product and associated with a list of rules, that is used to decrypt the list of rules so that a user may gain rule-based access to information associated with the packaged product (¶224).

In summary, Schneck teaches that the cryptographically sealed certificate includes a decryption key that may be used to decrypt a rule-encrypting key K_R . Once K_R is obtained, it may be applied to decrypting a data key K_D that is integrated within a packaged product so the information content of the packaged product may be subsequently decrypted with the data key K_D .

Schneck does not teach or suggest the claimed feature of selecting keys, algorithms, and reference parameters associated

with a certificate based on a unique device name contained in the certificate. Although, as noted in section 7.2 of the Office Action, Schneck discloses that the rule-encrypting key K_R may be determined as a function of a validated system serial number ($K_R=f(SN)$) and this function may take the form of an inquiry to a certification database to obtain the public key, Schneck does not disclose obtaining the validated system serial number from the certificate. Moreover, Schneck does not disclose selecting multiple keys based on the serial number or selecting cryptographic algorithms and reference parameters based on the serial number. Instead, Schneck simply discloses decrypting the rule-encrypting key K_R using a decryption key included in the certificate.

Accordingly, Applicants submit that the combined teachings of Thomlinson and Schneck do not render obvious the subject matter of claim 13. Claims 31 and 33 similarly recite the feature distinguishing claim 13 from Thomlinson and Schneck. Therefore, allowance of claims 13, 31, and 33 and all claims dependent therefrom is warranted.

Regarding claim 26, the Office Action proposes that Schneck discloses, in paragraphs 279-281, generating a digital signature of a unique device name using a private key. However, the cited portion of Schneck discloses generating a digital signature to

accompany quoted text that is extracted from a source. Although the digital signature includes a unique device name, a digital signature of the device name is not created. Moreover, Schneck does not teach that a key is involved in creating the digital signature.

The Office Action proposes that Schneck discloses, in paragraph 279, producing a second intermediate result from a first intermediate result using a shared secret key. The cited paragraph does not mention a key and, therefore, cannot disclose the specific features attributed to it.

The Office Action proposes that Schneck discloses concatenating first and second intermediate results to produce a certificate. However, the cited paragraph only discloses, with regard to the certificate, that the certificate includes a key. Moreover, Schneck only discloses, with regard to the content of the certificate, that the certificate is cryptographically sealed and includes a decryption key (Schneck ¶187), no other specific contents of the certificate are described. As a result, it necessarily follows that Schneck cannot disclose concatenating the specific features recited in claim 26 to produce the certificate.

As apparently noted in the office action, Chasko does not supplement the teachings of Schneck with regard to the above-mentioned features distinguishing claim 26 from Schneck.

Accordingly, Applicants submit that the applied references do not suggest the subject matter defined by claim 26. Therefore, allowance of claim 26 and all claims dependent therefrom is warranted.

Regarding claim 27, the Office Action proposes that Schneck discloses, in paragraph 188, a certificate containing a plain text device name and a signed device name. An examination of this paragraph reveals that Schneck does not teach these features therein. By contrast to the proposed disclosure, Schneck only teaches, with regard to the content of the certificate, that the certificate is cryptographically sealed and includes a decryption key (Schneck ¶187).

The Office Action further proposes that Schneck discloses, in paragraph 281, cross-referencing a device name obtained from a certificate with keys, cryptographic algorithms, and reference parameters. The discussion provided above in connection with claim 13 evinces that Schneck does not disclose the proposed features.

Schneck also does not disclose verifying a signed device name contained in a certificate, as proposed in the Office

Action. This necessarily follows because Schneck does not disclose a certificate containing a signed device name.

Similarly, Schneck cannot disclose comparing a resulting device name with a device name in a certificate, as proposed in the Office Action, because Schneck does not disclose a certificate containing a device name. Moreover, Schneck cannot disclose performing an authentication code function on the above-described features attributed, by the Office Action, to the certificate because Schneck does not disclose a certificate having these features.

Schneck does not disclose comparing anything in paragraphs 271, 279, and 281, as proposed in the Office Action. Therefore, it necessarily follows that these paragraphs cannot teach comparing the specific features recited in claim 27.

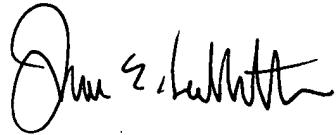
Nakamura is not cited for teaching any of the features cited above for distinguishing claim 27 from Schneck.

Accordingly, Applicants submit that the applied references do not suggest the subject matter defined by claim 27. Therefore, allowance of claim 27 and all claims dependent therefrom is warranted.

In view of the above, it is submitted that this application is in condition for allowance and a notice to that effect is respectfully solicited.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,



James E. Ledbetter
Registration No. 28,732

Date: February 11, 2005
JEL/DWW/att

Attorney Docket No. L741.01105
STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, N.W., Suite 850
P.O. Box 34387
Washington, D.C. 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200